What is claimed is:

1. A method for detecting and removing malicious code from a computer system, comprising:
determining an operating system of the computer system;
scanning the computer system for malicious code based on the determined operating system; and
detecting the malicious code.

2. The method of claim 1, further comprising:
removing the malicious code from the computer system.

3. The method of claim 1, further comprising displaying a message to a user identifying the malicious code.

4. The method of claim 1, further comprising displaying a message to a user indicating the presence of malicious code in the computer system.

5. The method of claim 1, wherein the removing step further comprises retrieving from a data file, information relating to the detected malicious code, including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code and executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code.

6. The method of claim 5, wherein the data file is retrieved based on a command from the user.

7. The method of claim 1, wherein the scanning step further comprises scanning a memory of the computer system in accordance with a memory layout associated with the determined operating system.

8. The method of claim 1, wherein the scanning step comprises dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

9. The method of claim 6, wherein selected memory blocks are not scanned in accordance with the determined operating system.

10. A storage medium including computer executable code for detecting and removing malicious code from a computer system, comprising:

code for determining an operating system of the computer system;

code for scanning the computer system for malicious code based on the determined operating system; and

code for detecting the malicious code.

11. The storage medium of claim 10, further comprising:

code for removing the malicious code from the computer system.

12. The storage medium of claim 10, further comprising code for displaying a message to a user identifying the malicious code.

13. The storage medium of claim 10, further comprising code for displaying a message to a user indicating that the malicious code is present on the computer system.

14. The storage medium of claim 10, wherein the code for removing the malicious code further comprises:

code for retrieving from a data file, information relating to the malicious code including at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code and executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code after the message identifying the malicious code is displayed to the user.

15. The storage medium of claim 14, wherein the code for retrieving is implemented in response to a command from a user.

16. The storage medium of claim 10, wherein the code for scanning further comprises code for scanning a memory of the computer system according to a memory layout associated with the determined operating system.

17. The storage medium of claim 10, wherein the code for scanning further comprises code for dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

18. The storage medium of claim method of claim 17, wherein the code for scanning further comprises code for determining selected memory blocks that are not scanned in accordance with the determined operating system.

19. A computer data signal embodied in a transmission medium and including computer executable instructions for detecting and removing malicious code from a computer system, comprising:

a data signal portion for determining an operating system of the computer system;

a data signal portion for scanning the computer system for malicious code based on the determined operating system; and

a data signal portion for detecting the malicious code.

20. The computer data signal of claim 19, further comprising:

a data signal portion for removing the malicious code.

21. The computer data signal of claim 19, further comprising a data signal portion for

displaying a message to a user identifying the malicious code.

22. The computer data signal of claim 19, further comprising a data signal portion for displaying a message indicating to a user that malicious code is present in the computer system.

23. The computer data signal of claim 19, wherein the data signal portion for removing the malicious code further comprises:

a data signal portion for retrieving from a data file, information relating to the malicious code including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code and a data signal portion for executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code.

24. The computer data signal of claim 23, wherein the data file is retrieved in response to a command from a user.

25. The computer data signal of claim 19, further comprising a data signal portion for scanning a memory of the computer system in accordance with a memory layout associated with the determined operating system.

26. The computer data signal of claim 19, wherein the data signal portion for scanning further comprising a data signal portion for dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

27. The computer data signal of claim 26, wherein the data signal portion for scanning further includes a data signal portion for determining selected memory blocks that are not scanned, based on the determined operating system.

28. A system for detecting and removing malicious code from a computer system, comprising:

an identifying device adapted to determine an operating system of the computer system;

a scanning device adapted to scan the computer system for malicious code based on the determined operating system; and

a code identifying device adapted to detect the malicious code.

29. The system of claim 28, further comprising:

a code removal device adapted to remove the malicious code from the computer system.

30. The system of claim 28, further comprising a display device adapted to display a message to a user identifying the malicious code.

31. The system of claim 28, further comprising a display device adapted to display a message indicating to a user that malicious code is present on the computer system.

32. The system of claim 28, wherein the code removal device further comprises: a retrieving device adapted to retrieve, from a data file, information relating to the malicious code including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code and an execution device adapted to execute the at least one command for restoring the computer system to substantially the same state as it existed prior to modification by the malicious code.

33. The system of claim 32, wherein the data file is retrieved in response to a command from a user.

34. The system of claim 28, wherein the scanning device further scans a memory of the computer system in accordance with a memory layout associated with the determined operating system.

35. The system of claim 28, wherein the scanning device divides memory locations of the computer system into a plurality of memory blocks and scans predetermined memory blocks in accordance with the determined operating system.

36. The system of claim 35, wherein the scanning device does not scan selected memory blocks based on the determined operating system.